Научная статья
УДК 004.056.5; DOI: 10.61260/2218-13X-2023-4-109-118

КАТЕГОРИРОВАНИЕ И МАРКИРОВКА ДОКУМЕНТОВ КАК МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ (НА ОПЫТЕ США)

✉**Метельков Александр Николаевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***metelkov5178@mail.ru***

Аннотация. В последние годы отмечается резкий рост таргетированных компьютерных атак на информационные ресурсы Российской Федерации и предприятий, отдельных организаций. В этих условиях существенно актуализируется проблема защиты информации, обрабатываемой в цифровой форме в государственных информационных системах и информационных системах персональных данных. Эта проблема аккумулирует опыт освоения информационных технологий в развитых странах, носит междисциплинарный характер и поэтому изучается техническими, юридическими и другими науками. В работе автором на основе открытых публикаций обобщены сведения о подходе США и других стран Запада к защите несекретной контролируемой информации. В статье с использованием анализа официальных документов об обеспечении безопасности информации выделен сложноструктурированный подход к дифференциации защищаемой несекретной информации, ее специальной маркировке, что позволяет осуществлять «сквозной» контроль над обращением информации в период всего ее жизненного цикла существования. Изучение опыта США в области защиты информации в информационных системах позволяет углубить понимание содержания и форм сведений конфиденциального характера, уточнить направления развития и скорректировать методы защиты служебной информации ограниченного распространения.

Ключевые слова: информация, защита информации, несекретная контролируемая информация, контролируемая среда, уровень контроля, средства контроля, маркировка

Для цитирования: Метельков А.Н. Категорирование и маркировка документов как метод защиты информации в информационных системах (на опыте США) // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 4. С. 109–118. DOI: 10.61260/2218-13X-2023-4-109-118.

Scientific article

CATEGORY AND LABELING OF DOCUMENTS AS A METHOD OF INFORMATION PROTECTION IN INFORMATION SYSTEMS (US EXPERIENCE)

✉**Metel'kov Alexander N.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***metelkov5178@mail.ru***

Abstract. In recent years, there has been a sharp increase in targeted computer attacks on the information resources of the Russian Federation and enterprises and individual organizations. In these conditions, the problem of protecting information processed in digital form in government information systems and personal data information systems is significantly updated. This problem accumulates the experience of mastering information technologies in developed countries, is interdisciplinary in nature and is therefore studied by technical, legal and other sciences. Based on open publications, the author summarizes information about the approach of the United States and other Western countries to the protection of unclassified controlled information. Using the analysis of official

documents on information security, the article highlights a complex structured approach to the differentiation of protected unclassified information, its special labeling, which allows for «end-to-end» control over the circulation of information during its entire life cycle of existence. Studying the US experience in the field of information security in information systems allows us to deepen our understanding of the content and forms of confidential information, clarify the directions of development and adjust the methods of protecting official information of limited distribution.

Keywords: information, information protection, unclassified controlled information, controlled environment, level of control, controls, labeling

For citation: Metel'kov A.N. Category and labeling of documents as a method of information protection in information systems (US experience) // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 4. P. 109–118. DOI: 10.61260/2218-13X-2023-4-109-118.

Введение

В Стратегии национальной безопасности Российской Федерации [1] информационная безопасность определена в числе стратегических национальных приоритетов в обеспечении и защите национальных интересов Российской Федерации, на реализации которых концентрируются усилия и ресурсы органов публичной власти, организаций и институтов гражданского общества. Обеспечению приоритетного использования в информационной инфраструктуре российских информационных технологий, отвечающих требованиям информационной безопасности при реализации национальных проектов и решении задач в области цифровизации государственного управления, способствует совершенствование методов и средств защиты информации. Для технической защиты конфиденциальной информации используются различные аппаратно-программные и программные средства защиты конфиденциальной информации (антивирусы, межсетевые экраны, прокси-серверы, VPN, DLP-системы, IDS-системы, IPS- и SIEM-системы и др.) зарубежных и отечественных производителей.

Соблюдение Требований к организации защиты информации, содержащейся в информационной системе [2] требует точного и полного выделения объектов технической защиты в государственных информационных системах, включая саму защищаемую информацию. В условиях бурного развития информационно-коммуникационных технологий и увеличения числа угроз безопасности информации рост числа компьютерных атак с территорий иностранных государств на российские информационные ресурсы требует обеспечения устойчивости и безопасности всех элементов цифровой информационной инфраструктуры государственных органов и иных субъектов оборота цифровых данных. Проблема структурирования конфиденциальной информации и контроля за оборотом цифровых данных с увеличением их объемов приобретает особую актуальность.

Методы исследования

Процесс развития информационного общества в государствах взаимосвязан и взаимозависим. Отечественные информационные технологии, направленные на защиту цифрового суверенитета, развиваются в условиях общемировых тенденций и технологий в сфере защиты информации. Особое внимание в этом развитии занимает понимание защищаемой информации, методов, способов и приемов ее защиты. Некоторые подходы отражены в работах [3–5]. В этом контексте полезно изучение мирового опыта. На основе анализа концептуальных подходов и обобщения опыта защиты несекретной контролируемой информации в США методами ее структурирования, категорирования и маркирования автором предлагается осмыслить эти подходы для их возможного использования при защите конфиденциальных сведений в России. В российских нормативных правовых актах [6–9] и других документах для описания требующей защиты несекретной информации используются термины: «служебная информация ограниченного распространения», «служебная информация ограниченного доступа», «служебная информация с ограниченным доступом»,

«конфиденциальная информация», «сведения конфиденциального характера» и др. В научной среде по поводу их содержания ведутся дискуссии. Соотношение и упорядочивание этих терминов не проводится, что затрудняет оборот цифровой информации и является существенным препятствием для ее защиты.

Маркирование категорированных документов в США как способ защиты несекретной контролируемой информации

В Доктрине информационной безопасности Российской Федерации [9] информация включена в понятие информационной сферы, наряду с объектами информатизации, информационными системами, сайтами в сети Интернет, сетями связи, информационными технологиями, субъектами, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности. В российском законодательстве, руководящих документах государственных регуляторов и на практике конфиденциальная информация понимается как определенная категория сведений, доступ к которым ограничен. В странах с англо-американской правовой системой существует довольно схожее толкование того, какую информацию считать конфиденциальной [10]. Сравнительно-исторический подход к исследованию законодательства о коммерческой тайне и конфиденциальной информации в обеих странах показывает, что изменения в канадском законодательстве повторяют американские [11]. В европейских странах имеется специфика защиты аналогичной информации. В Общем регламенте защиты данных (General Data Protection Regulation, GDPR) Европейского Союза и его национальных адаптациях информация об обработке играет решающую роль для субъектов данных. В European Data Protection Board к передовым практикам отнесены следующие:

– информация должна предоставляться в простой и понятной форме, избегая «сложных предложений и языковых структур»;

– информация должна быть однозначной, в том смысле, что не должна оставлять места для различных интерпретаций;

– следует избегать расплывчатых формул;

– текст должен быть четко и логично структурирован (с использованием маркеров и отступов);

– активная форма всегда должна быть предпочтительнее пассивной;

– следует избегать, насколько это возможно, узкотехнических или специализированных выражений (в том числе «юридических»);

– в случае многоязычных уведомлений о политике все языковые версии должны быть последовательными и ясными;

– всегда должна быть доступна версия на языке субъекта данных.

В США после теракта 11 сентября 2001 г. были приняты системные меры по защите информации. В частности, разработана Программа контролируемой несекретной информации исполнительной власти (Программа CUI), в которой была установлена политика определения, обработки и снятия с контроля такой информации. Программа CUI, учрежденная Президентом США в Исполнительном приказе от 4 ноября 2010 г. № 13556, выполняется во всех агентствах и департаментах исполнительной власти. Программа CUI стандартизирует порядок обработки защищаемой информации. CUI – это несекретная информация, требующая защиты и контроля за распространением в соответствии с применимыми законами, постановлениями и общегосударственной политикой. Например, информация об уязвимостях информационных систем, общая информация о критической инфраструктуре, сведения об управлении в чрезвычайных ситуациях в США отнесены к CUI. Хотя эта информация не засекречена, агентства все равно должны обращаться с ней в соответствии с требованиями Федерального закона о модернизации информационной безопасности (FISMA). До принятия Программы CUI агентства США использовали

специальные политики, процедуры и маркировку для обработки такой информации. Этот лоскутный подход приводил к непоследовательной обработке информации, применению нечеткой или излишне ограничительной политики распространения и созданию препятствий для обмена информацией. Политика CUI в масштабах всей исполнительной власти уравновешивает необходимость защиты CUI в обмене информацией с общественными интересами без лишних обременений. Политика не применяется к организациям, не относящимся к исполнительной власти, но косвенно относится к получателям CUI путем включения в соответствующие соглашения (контракты, гранты, лицензии, сертификаты, меморандумы о договоренности или взаимопонимании, соглашения об обмене информацией). Совместное использование CUI разрешено для любой государственной цели, которая представляет собой любую деятельность, миссию, функцию или операцию, признаваемые Правительством США, входящей в сферу своих законных полномочий. Программа CUI обеспечит своевременный и последовательный обмен информацией, одновременно улучшая защиту конфиденциальной информации в федеральном правительстве и среди заинтересованных нефедеральных сторон. Федеральные агентства США регулярно генерируют, используют, хранят и передают информацию, которая, хотя и не засекречена, все же требует определенного уровня защиты от несанкционированного доступа и разглашения. Обработка – это любое использование CUI, включая маркировку, защиту, транспортировку, распространение, повторное использование и уничтожение информации. Приказом № 13556 введено понятие «исполнительный агент», которому поручено разрешить конфликты между категориями и подкатегориями CUI для достижения единообразия в маркировке информации. Исполнительным агентом CUI (EA) определено Национальное управление архивов и документации (NARA), реализующее программу CUI для исполнительной власти и контролирующее действия федеральных агентств. NARA делегировало эти полномочия директору Управления по надзору за информационной безопасностью (ISOO). Исполнительный агент после консультации с заинтересованными ведомствами издает директивы, необходимые для выполнения требований Приказа № 13556. Такие директивы должны быть доступны общественности и предусматривать политику и процедуры, касающиеся маркировки, охраны, распространения и снятия с контроля CUI, которые должны оставаться согласованными для всех категорий CUI и для всех органов исполнительной власти.

Федеральная CUI разделена на несколько категорий и подкатегорий и внесена в реестр CUI, которым управляет Национальное управление архивов и документации (NARA). CUI по определению является федеральной информацией. CUI определяется в Исполнительном указе Президента США № 13556 как информация, хранящаяся или созданная для федерального правительства, защита или распространение которой требует контроля в соответствии с действующим законодательством, постановлениями и общегосударственной политикой и не классифицируется в соответствии с Приказом № 13526 или Законом об атомной энергии с поправками. Категория «контролируемая несекретная информация» делится на два подмножества: базовое и специальное. Базовое (CUI Basic) – это подмножество CUI, для которого разрешающий закон, постановление или общегосударственная политика не устанавливает конкретных мер контроля за обращением или распространением. Специальное или указанное (CUI Specified) – это подмножество CUI, для которого санкционирующий закон, постановление или общегосударственная политика определяет агентствам требования или разрешения, отличающиеся от используемых для CUI Basic, к используемым средствам управления обработкой. К некоторым типам защищаемой информации в законах устанавливаются особые требования к их защите. Например, информация, связанная с экспортом. При условии соблюдения требований конфиденциальности согласно Закону об экспортном контроле 1979 г. с поправками (EAR) и Закону о защите конфиденциальной информации и статистической эффективности (CIPSEA) с этими сведениями нельзя обращаться таким же образом, как с и подавляющим большинством других типов CUI. Все CUI, для которых законом, постановлением или

общегосударственной политикой не предусмотрена защита, попадают в базовые категории CUI Basic. Защита включает в себя все меры контроля, которые агентство применяет или должно применять при обработке информации, которая квалифицируется как CUI. Все категории базового CUI будут контролироваться единому стандарту – не ниже «умеренной» конфиденциальности, минимально возможного уровня контроля, то есть выше «низкого» стандарта, уже применяемого ко всем информационным системам без CUI. Базовые требования – это требования по умолчанию для защиты CUI, применяемые к подавляющему большинству CUI. Однако к некоторым категориям и подкатегориям CUI могут предъявляться более высокие или отличные от базовых требования, если закон, постановление или общегосударственная политика требуют или разрешают другие меры контроля для защиты или распространения такой информации. CUI Specified в отличие от CUI Basic, распознает типы CUI, которые имеют обязательные или разрешенные элементы управления, включенные в их регулирующие полномочия. Каждая категория или подкатегория CUI Specified применяет эти элементы управления в соответствии с требованиями или разрешениями регулирующего закона, постановления или политики. Сведения, получаемые в результате частных исследований, которые федеральное правительство не финансирует, даже несмотря на то, что они подпадают под действие правил экспортного контроля США, не относятся к CUI. Проекты, включающие контролируемую информацию, не относящуюся к CUI, могут обрабатываться с соблюдением тех же стандартов защиты, но не должны быть помечены как CUI. Неконтекстуализированные данные контролируемых исследований – это такие данные, созданные в рамках проекта с требованиями защиты CUI, которые контролируются и должны обрабатываться в соответствии с соответствующим Планом контроля технологий (TCP), но это не CUI. В США для защиты CUI используются меры защиты информации от несанкционированного доступа или случайного публичного раскрытия. Это требование включает, но не ограничивается:

– хранением CUI в среде, предотвращающей несанкционированный доступ, например, в помещениях/зонах и онлайн-хранилище (для электронных CUI) с контролем доступа;

– предотвращением физического доступа путем хранения документов CUI в запертых шкафах и ящиках;

– хранением электронной CUI в соответствии с требованиями, установленными в публикации NIST 800–171, посвященной защите CUI в нефедеральных системах и организациях.

Для категорирования несекретной конфиденциальной информации CUI предусматривается ее маркировка в соответствии с Руководством по маркировке, выпущенным NARA. Маркировка категории или подкатегории CUI – это маркировка, утвержденная Исполнительным агентом CUI (EA) для категорий и подкатегорий, перечисленных в реестре CUI. Распространение CUI предусматривается только уполномоченным лицам при соблюдении требований NARA по снятию с контроля и уничтожению CUI.

Защита контролируемой несекретной информации может потребоваться в целях конфиденциальности, соблюдения закона, договорной защиты или по другим причинам. Исторически сложилось так, что каждое агентство разрабатывало свои собственные методы работы с конфиденциальной информацией, что привело к разбросу процессов в федеральных агентствах. Подобная информация может быть помечена по-разному, разные типы информации могут иметь одинаковую маркировку с разным значением в зависимости от ее использования в каждой организации. Программа CUI была призвана стандартизировать способы, которыми правительство и различные организации, взаимодействующие с Министерством обороны, обрабатывают и защищают несекретную информацию. До действующей программы CUI каждое агентство использовало свой набор маркировки (FOUO, LES, SBU, UCTI и т.д.), классификацию информации и правила

управления и контроля информации. Многие организации аэрокосмической и оборонной промышленности, возможно, привыкли к маркировке, наносимой на такие данные, как: только для официального использования (FOUO); чувствительный к правоохранительным органам (LES); конфиденциально, но несекретно (SBU); несекретная контролируемая техническая информация (UCTI) и т.д. Все эти категории стали называться контролируемой несекретной информацией или CUI. Эта информация, хотя и не является секретной, по-прежнему имеет решающее значение для национальной обороны США и требует особой защиты для предотвращения несанкционированного доступа или раскрытия. В 2023 г. Министерство обороны США завершает процесс нормотворчества, фактически включив пункт 252.204–7021 DFARS в положение о контрактах с Министерством обороны, в результате которого при заключении контрактов сотрудники смогут включить этот пункт к нисходящим требованиям сертификации модели зрелости кибербезопасности (CMMC) в своих цепочках поставок.

В терминологическом аппарате защиты информации в США следует выделить понятия «контролируемая несекретная информация», «контролируемая среда», «уровень контроля», «средства контроля». Контролируемая несекретная информация – это информация, которую создают или которой обладают Правительство США или организация для Правительства или по его поручению, и с которой закон, нормативные акты или общегосударственная политика требуют или разрешают агентству обращаться с использованием средств защиты или контроля распространения. Однако CUI не включает секретную информацию или информацию, которой обладает и поддерживает в своих собственных системах организация, не относящаяся к исполнительной ветви власти, которая не поступила от организации, не была создана или которой владеет организация или для нее орган исполнительной власти или юридическое лицо, действующее от имени агентства. Закон, нормативные акты или общегосударственная политика могут требовать или разрешать учреждениям контроль за сохранностью или распространением тремя способами:

– контролировать или защищать информацию, но не предусматривать конкретных мер контроля, что делает информацию базовой CUI Basic;

– контролировать или защищать информацию и обеспечивать конкретные меры контроля за выполнением, что делает информацию CUI Specified;

– контролировать только указанную информацию, что делает информацию CUI Specified, но с базовыми элементами управления CUI, которые не определены уполномоченным органом.

Контролируемая среда – это любая область или пространство, которое, по мнению уполномоченного владельца, имеет адекватные физические или процедурные средства контроля (например, барьеры или управляемый контроль доступа) для защиты CUI от несанкционированного доступа или раскрытия. Средства контроля – это средства защиты или распространения, которые закон, нормативные акты или общегосударственная политика требуют или разрешают агентствам использовать при обработке CUI.

Уровень управления – это общий термин, обозначающий требования к защите и распространению, связанные с базовым CUI Basic и заданным CUI Specified. Агентства обрабатывают CUI Basic в соответствии с единым набором средств контроля и реестром CUI. Элементы управления CUI Basic применяются всякий раз, когда указанные CUI элементы управления не охватывают CUI Specified.

Маркировка является первым шагом в правильном обращении с CUI, поскольку она предупреждает держателей о необходимости защиты информации. Например, ряд кодов маркировок CUI приведен в табл. 1.

Таблица 1

Маркировка различных категорий CUI

Маркировка	Категория информации
CUI//SP-CEI	Информация о критической энергетической инфраструктуре
CUI//SP-CTI	Контролируемая техническая информация
CUI//SP-FNC	Общая финансовая информация
CUI//SP-GENETIC	Генетическая информация
CUI//SP-HLTH	Медицинская информация
CUI//SP-LDNA	ДНК
CUI//SP-PCII	Информация о защищенной критической инфраструктуре
CUI//SP-PERS	Кадровые записи
CUI//SP-PROCURE	Общие закупки и комплектование
CUI//SP-PRVCY	Общая конфиденциальность
CUI//SP-SSI	Конфиденциальная информация безопасности
CUI//SP-STUD и др.	Учетные записи студентов

CUI связан с соблюдением требований NIST и сертификации модели зрелости кибербезопасности (CMMC). Существуют также две категории, специфичные для НАТО, которые считаются указанными, но не имеют маркировки по умолчанию (Ограниченный НАТО и Несекретный НАТО), конкретная маркировка которых будет зависеть от содержимого соответствующего документа. Существует несколько категорий CUI, определенных Министерством обороны США (DoD), включая CTI, SP-DCNI и SP-NNPI. В случае обработки любой из них пользователь может столкнутся с базовой категорией информации о безопасности критической инфраструктуры Министерства обороны США (DCRIT). Помимо маркировок, CUI Specified часто требует дополнительных обозначений для элементов управления, таких как Limited Dissemination. Например, документы могут требовать маркировки «NF», если они не разрешены для распространения за рубежом. Документы (их разделы) могут маркироваться обозначением «FEDCON», если доступ к ним разрешен только федеральным служащим и подрядчикам. На ряд категорий CUI Specified помимо обязательной маркировки документов, определенных как CUI, распространяются специальные правила агентства по их совместному использованию, хранению, обработке и т.д. Некоторые из них имеют только один руководящий орган или структуру, в то время как другие могут подчиняться сразу нескольким одновременно. Например, категория BUDG подпадает под действие циркуляра OMB A-11, раздел 22.1. Этот документ определяет средства контроля за распространением и защитой, выходящие за рамки того, что требуется для всех CUI.

Документы и электронные файлы, содержащие CUI, должны быть маркированы в соответствии с Руководством по маркировке CUI. Все CUI должны быть помечены как таковые. Категории CUI группируются с помощью организационных индексов, как, например, показано в табл. 2 применительно к группам «критическая инфраструктура» и «защита».

Специальная маркировка CUI Specified используется для категорий, указанных в CUI. Маркировка всегда включает «Контролируемый» или «CUI», а маркировка «CUI Specified», в частности, также требует кода для обозначения указанной категории. Если CUI Basic, он должен включать баннер «CONTROLLED» или «CUI». Если указан CUI, он должен включать конкретные полномочия.

На практике организации отслеживают различные структуры и правила безопасности, применимые к конкретному виду CUI, который они обрабатывают. В конечном счете, обеспечение безопасности CUI не означает определение того, какой уровень конфигурации системы и сети необходим для CUI в целом. Вместо этого речь идет о внедрении конкретных рамок и средств контроля, разработанных властями, занимающимися конкретными категориями CUI. Федеральные правила сортируют CUI по длинному списку категорий и подкатегорий. Наиболее часто используемые категории CUI представлены в табл. 3.

Таблица 2

Группы организационных индексов по категории CUI

Группы организационных индексов	Категории CUI
Критическая инфраструктура	Защищенная информация о критической инфраструктуре Информация об уязвимостях информационных систем Информация об уязвимости химического терроризма Информация о критической энергетической инфраструктуре Информация о Законе о безопасности Нитрат аммония Общая информация о критической инфраструктуре Оценка воды Токсические вещества Управление в чрезвычайных ситуациях Физическая охрана
Защита	Контролируемая техническая информация Информация о безопасности критической инфраструктуры Министерства обороны США Информация о военно-морских ядерных двигательных установках Несекретная контролируемая ядерная информация – Оборона

Таблица 3

Кодирование категорий CUI в зависимости от видов

Вид	Уровень	Условное обозначение (кодирование)	Категория CUI: (по требованиям Национального архива США)
Экспортный контроль	Базовый или указанный	CUI//SP-EXPT	Экспортный контроль
Экспортно-контролируемые исследования	Базовый	CUI//SP- EXPTR	Исследования, контролируемые экспортом
Информация о здоровье	Базовый или указанный	CUI//SP-HLTH	Информация о здоровье
Контролируемая техническая информация	Указанный	CUI/SP-CTI	Контролируемая техническая информация

Заключение

Стремительное развитие информационных технологий и телекоммуникационных сетей способствует быстрому накоплению значительных объемов несекретной информации, в том числе требующей защиты. Объективно существует потребность в ее структурировании и идентификации на основе отнесения к определенным категориям, что обеспечивает гибкость в применении организационно-технических методов и средств. Опыт защиты конфиденциальной информации в США с присвоением меток для идентификации ее различных категорий заслуживает внимания, дальнейшего изучения и возможного использования в государственных информационных системах защиты информации в России. В результате исследования автор приходит к выводу о возможности адаптации метода категорирования сведений конфиденциального характера и защищаемой служебной информации в качестве одного из перспективных направлений в обеспечении безопасности информации.

Список источников

1. О Стратегии национальной безопасности Российской Федерации: Указ Президента Рос. Федерации от 2 июля 2021 г. № 400 // Собр. законодательства Рос. Федерации. 2021. № 27 (Ч. II). Ст. 5351.

2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ Федеральной службы по техническому и экспортному контролю от 11 февр. 2013 г. № 17 (в ред. приказа Федеральной службы по техническому и экспортному контролю от 28 мая 2019 г. № 106) // Рос. газ. 2013. № 136. 26 июня.

3. Линьков В.В., Грунин И.Ю., Дубов С.С. Предотвращение утечек конфиденциальной информации из информационной системы вовне // Путь науки. 2019. № 8 (66). С. 14–22.

4. Митюшин Д.А. Правовые вопросы применения систем защиты от утечки конфиденциальной информации на объектах информатизации // Вестник Московского университета МВД России. 2020. № 5 (35). С. 163–168.

5. Шивдяков Л.А. Защита конфиденциальной информации в автоматизированных системах // Безопасность информационных технологий. 2008. Т. 15. № 1. С. 110–114.

6. Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 29 дек. 2022 г.) // Собр. законодательства Рос. Федерации. 2006. № 31. Ст. 3448.

7. О персональных данных: Федер. закон от 27 июля 2006 г. № 152-ФЗ (в ред. от 6 февр. 2023 г.) // Собр. законодательства Рос. Федерации. 2006. № 31 (Ч. I). Ст. 3451.

8. Об утверждении Перечня сведений конфиденциального характера: Указ Президента Рос. Федерации от 6 марта 1997 г. № 188 // Собр. законодательства Рос. Федерации. 1997. № 10. Ст. 1127.

9. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

10. Капустина А.Г. Зарубежная практика регулирования конфиденциальной информации // Защита информации. Инсайд. 2010. № 5 (35). С. 24–26.

11. Malone Matt. A Comparative History of the Law of Confidential Information and Trade Secrets in Canada and the United States: Towards Harmonization? // 34:1 Intellectual Property Journal (Forthcoming, 2022). Available at SSRN: https://ssrn.com/abstract=3949074.

References

1. O Strategii nacional'noj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 2 iyulya 2021 g. № 400 // Sobr. zakonodatel'stva Ros. Federacii. 2021. № 27 (Ch. II). St. 5351.

2. Ob utverzhdenii Trebovanij o zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah: prikaz Federal'noj sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 11 fevr. 2013 g. № 17 (v red. prikaza Federal'noj sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 28 maya 2019 g. № 106) // Ros. gaz. 2013. № 136. 26 iyunya.

3. Lin'kov V.V., Grunin I.Yu., Dubov S.S. Predotvrashchenie utechek konfidencial'noj informacii iz informacionnoj sistemy vovne // Put' nauki. 2019. № 8 (66). S. 14–22.

4. Mityushin D.A. Pravovye voprosy primeneniya sistem zashchity ot utechki konfidencial'noj informacii na ob"ektah informatizacii // Vestnik Moskovskogo universiteta MVD Rossii. 2020. № 5 (35). S. 163–168.

5. Shivdyakov L.A. Zashchita konfidencial'noj informacii v avtomatizirovannyh sistemah // Bezopasnost' informacionnyh tekhnologij. 2008. T. 15. № 1. S. 110–114.

6. Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii: Feder. zakon ot 27 iyulya 2006 g. № 149-FZ (v red. ot 29 dek. 2022 g.) // Sobr. zakonodatel'stva Ros. Federacii. 2006. № 31. St. 3448.

7. O personal'nyh dannyh: Feder. zakon ot 27 iyulya 2006 g. № 152-FZ (v red. ot 6 fevr. 2023 g.) // Sobr. zakonodatel'stva Ros. Federacii. 2006. № 31 (Ch. I). St. 3451.

8. Ob utverzhdenii Perechnya svedenij konfidencial'nogo haraktera: Ukaz Prezidenta Ros. Federacii ot 6 marta 1997 g. № 188 // Sobr. zakonodatel'stva Ros. Federacii. 1997. № 10. St. 1127.

9. Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 5 dek. 2016 g. № 646 // Sobr. zakonodatel'stva Ros. Federacii.2016. № 50. St. 7074.

10. Kapustina A.G. Zarubezhnaya praktika regulirovaniya konfidencial'noj informacii // Zashchita informacii. Insajd. 2010. № 5 (35). S. 24–26.

11. Malone Matt. A Comparative History of the Law of Confidential Information and Trade Secrets in Canada and the United States: Towards Harmonization? // 34:1 Intellectual Property Journal (Forthcoming, 2022). Available at SSRN: https://ssrn.com/abstract=3949074.

Информация о статье:
Статья поступила в редакцию: 13.11.2023; одобрена после рецензирования: 09.12.2023;
принята к публикации: 11.12.2023
Information about the article:
The article was submitted to the editorial office: 13.10.2023; approved after review: 09.12.2023;
accepted for publication: 11.12.2023

Сведения об авторах:
Метельков Александр Николаевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат юридических наук, e-mail: metelkov5178@mail.ru, https://orcid.org/0000-0002-6113-8981, SPIN-код: 5990-6833

Information about the authors:
Metelkov Alexander N., associate professor of the department of applied mathematics and information technologies, Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of law, e-mail: metelkov5178@mail.ru, https: //orcid.org/0000-0002-6113-8981, SPIN: 5990-6833